Network transmission confidentiality method for mobile telephone

Patent Number: FR2716319
Publication date: 1995-08-18
Inventor(s): PATRICE HOEL
Applicant(s):: SAGEM (FR)
Requested Patent: FR2716319
Application Number: FR19940001680 19940215
Priority Number(s): FR19940001680 19940215
IPC Classification: H04L9/32 ; H04B7/26
EC Classification: H04L9/32B, H04Q7/38A
Equivalents:

Abstract

The method involves a unique data support device for each user and two authentication codes. The first is for access to the network and the other is for access to a service. The authentication codes must be verified before access is permitted. The network access code is numerically deducted from the service access code and is verified by comparison with the initial service access code. The system includes a service access module (33) and a network access module (4). The modules perform code deduction and access control operations.

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 716 319**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **94 01680**

(51) Int Cl⁶ : H 04 L 9/32, H 04 B 7/26

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 15.02.94.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande** : 18.08.95 Bulletin 95/33.

(56) **Liste des documents cités dans le rapport de recherche préliminaire** : *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés** :

(71) **Demandeur(s)** : *SOCIETE D'APPLICATIONS GENERALES D'ELECTRICITE ET DE MECANIQUE SAGEM société anonyme* — FR.

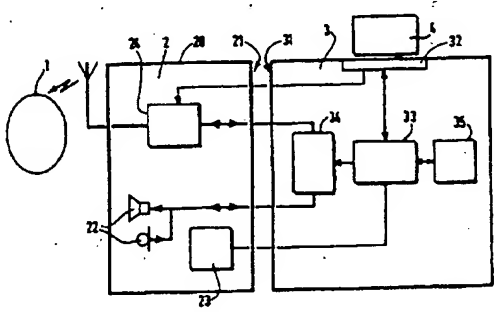
(72) **Inventeur(s)** : Hoel Patrice.

(73) **Titulaire(s)** :

(74) **Mandataire** : Bloch & Associés Conseils en Propriété Industrielle.

(54) Procédé de communication sur un réseau de transmission à double authentification et support de données pour la mise en œuvre du procédé.

(57) Procédé de communication sur un réseau de transmission, au moyen d'un support de données (3, 4) personnel à un utilisateur et à double code d'authentification, l'un (AB) pour l'accès au réseau, l'autre (XX) pour l'accès à un service, dans lequel on commence par saisir sur le support de données le code d'authentification de l'accès au service (XX) avant d'établir la communication par le code d'authentification de l'accès au réseau (AB) qui se déduit du code d'authentification de l'accès au service (XX).



FR 2 716 319 - A1

Procédé de communication sur un réseau de transmission à double authentification et support de données pour la mise en oeuvre du procédé.

La présente invention concerne tout d'abord un procédé de communication sur un réseau de transmission, au moyen d'un support de données personnel à un utilisateur et à double code d'authentification, l'un pour l'accès au réseau, l'autre pour l'accès à un service.

Certains réseaux de transmission d'informations nécessitent de disposer d'une autorisation pour y accéder. C'est par exemple le cas du réseau de téléphonie mobile GSM, pour lequel l'utilisateur doit préalablement s'identifier par connexion, au terminal GSM, d'une carte à puce personnelle qui, par paramétrage, peut n'être opérationnelle qu'après saisie d'un mot de code confirmant qu'il est bien un utilisateur autorisé de la carte.

En outre, les informations transmises sur le réseau de transmission (par exemple GSM/RTC), en général la parole, doivent parfois être protégées contre toute écoute illicite, c'est-à-dire subir un embrouillage avant émission et un débrouillage inverse en réception, la transmission embrouillée pouvant être assimilée à un service.

L'utilisateur doit alors accéder à un module d'embrouillage/débrouillage d'accès contrôlé, en général, par raccordement d'une autre carte à puce et saisie d'un autre mot de code afin de pouvoir connecter le module d'embrouillage/débrouillage entre lui-même et le réseau GSM. L'enchaînement de ces opérations d'authentification et d'accès est fastidieux et l'invention vise à le simplifier.

A cet effet, l'invention concerne un procédé du type défini ci-dessus, caractérisé par le fait qu'on commence par saisir sur le support de données le code d'authentification de l'accès au service avant d'établir la communication par le code d'authentification de l'accès au réseau qui se déduit du code d'authentification de l'accès au service.

Ainsi, pour l'utilisateur, on intègre l'autorisation d'accès au transport des informations et l'autorisation d'accès à leur traitement.

La communication sur le réseau, ou son accès, s'établit à l'autorisation de traitement. En d'autres termes, c'est cette autorisation de traitement qui émule l'autorisation d'accès, cette opération étant épargnée à l'utilisateur.

Avantageusement, le code d'authentification de l'accès au réseau se déduit du code d'authentification de l'accès au service par chiffrement pour empêcher de déduire ce code d'authentification du code d'authentification d'accès au réseau.

L'invention concerne aussi un support de données pour la mise en oeuvre du procédé de l'invention, comprenant un module d'accès au service et un module d'accès au réseau, caractérisé par le fait qu'il comporte des moyens agencés pour déduire une authentification de l'accès au réseau d'une authentification de l'accès au service et pour commander le module d'accès au réseau.

L'invention sera mieux comprise à l'aide de la description suivante de la forme de réalisation préférée d'un support de données pour la mise en oeuvre du procédé de l'invention, en référence à la figure unique du dessin annexé qui est une représentation schématique d'un terminal avec le support de données de l'invention.

Le terminal représenté schématique est raccordé à un réseau de transmission d'informations 1, ici le réseau de téléphonie mobile GSM.

Le terminal est constitué de deux parties, à savoir une partie combiné 2, purement téléphonique, d'interface avec le réseau 1 et une partie 3 de sécurisation des informations, la parole dans cet exemple, transmises à travers le réseau 1, c'est-à-dire de protection de la confidentialité de ces informations.

La partie de sécurisation 3, qui forme le module d'accès au service, est constituée d'un module amovible de faible taille, support de données, qui comporte un connecteur 31 coopérant avec un connecteur complémentaire 21 solidaire d'un boîtier 20 du combiné 2.

Pour la clarté du dessin, les connecteurs 21 et 31 ne sont figurés que par les bords en regard du boîtier 20 et du module 3.

Le module 3 comporte un autre connecteur, 32, pour recevoir une carte à puce 4, qui est le module d'accès au réseau.

Le connecteur 32 est relié à un circuit 33 de contrôle d'accès à un circuit 34 d'embrouillage/débrouillage de signaux de parole échangés, avec le réseau 1, par le combiné 2 au moyen d'un ensemble microphone et écouteur 22.

Le module 3 est ici, hormis ses connecteurs 31, 32, noyé dans une résine interdisant tout examen de ses circuits, afin d'en protéger un mot XX de code d'accès au service d'embrouillage/débrouillage, indiqué plus loin et mémorisé dans une mémoire 35 reliée au circuit 33.

Un clavier 23 du combiné 2, pour l'interface homme-machine, est relié, à travers le connecteur 21, 31, au circuit 33, dont une sortie commande le circuit 34.

Un bloc de communication 24 du combiné 2 est relié, par une liaison phonique bidirectionnelle représentée en trait renforcé, d'un côté, au réseau 1 et, de l'autre côté, à l'ensemble 22 à travers le circuit d'embrouillage/débrouillage 34.

La carte à puce 4 est aussi reliée directement au bloc de communication 24 par une liaison de commande traversant les connecteurs 32 et 21, 31. Dans cet exemple, la carte à puce est de format réduit, appelé micro-SIM (micro-module d'identification d'abonné).

Le fonctionnement du combiné 2-3 va maintenant être expliqué.

Comme déjà indiqué, il s'agit d'un procédé de communication sur le réseau 1 au moyen du module 3 de support de données personnel à un utilisateur et à double code d'authentification, l'une, AB, pour l'accès au réseau 1, l'autre, XX, pour l'accès au service (34) utilisant le réseau 1.

Dans une phase initiale de mise en service, le module 3 étant raccordé au combiné 2, on relie une carte de chargement de mot de code au connecteur 32 et on transfère ainsi, dans la mémoire 35, le mot de code secret XX d'autorisation d'accès au service d'embrouillage/débrouillage, c'est-à-dire d'accès au circuit 34. Le mot de code XX sert par la suite à authentifier l'utilisateur du combiné 2-3. A partir du mot de code XX d'accès au service d'embrouillage/débrouillage, ici par chiffrement, le circuit 33 calcule le mot de code AB d'accès au réseau 1. Dans cet exemple, on chiffre l'authentification de l'accès au service pour empêcher de déduire cette authentification de l'authentification d'accès au réseau AB déduite de l'authentification d'accès au service XX, c'est-à-dire que le chiffrement est choisi tel qu'il ne permet pas de remonter au mot de code XX à partir du mot de code AB. Dans une seconde phase de mise en service, la carte à puce 4 -module d'accès au réseau- est reliée au connecteur 32.

Le mot de code AB d'accès au réseau est lu par cette carte et est mémorisé, par des moyens externes classiques non représentés, dans la carte à puce 4.

En exploitation, l'utilisateur du combiné 2-3 dispose du combiné 2 proprement dit et il porte sur lui le module de sécurisation 3 ainsi que la carte 4 et, seul, il connaît le mot de code XX.

Pour établir une communication avec le réseau 1, l'utilisateur raccorde le module 3 au combiné 2 et insère la carte à puce 4 dans le connecteur 32. L'utilisateur compose ensuite le mot de code XX d'accès au service sur le clavier 23 et le circuit 33 le compare au mot de code XX d'accès au service mémorisé initialement dans la mémoire 35. En cas d'identité de ceux-ci, le circuit 33 autorise la mise en communication de l'ensemble microphone et haut-parleur 22 avec le bloc de communication 24, à travers le circuit d'embrouillage/débrouillage 34, c'est-à-dire qu'il valide l'accès au service.

Ensuite, on valide l'authentification de l'accès au réseau (AB) par comparaison à l'authentification initiale de l'accès au réseau (AB).

A cette fin, le circuit 33 engendre, ou déduit, par le même chiffrement du mot de code XX d'accès au service que dans la phase initiale, le mot de code AB

d'accès au réseau 1. Ce dernier mot de code AB est transmis à la carte à puce 4 qui, le comparant au mot de code d'accès au réseau 1 qui y a initialement été mémorisé, autorise le bloc de communication 24 à établir la liaison entre le réseau 1 et le circuit d'embrouillage/débrouillage 34.

Dans le cas où la carte 4 n'est pas celle qui est prévue, elle ne trouve pas d'identité entre les mots de code AB d'accès au réseau 1, respectivement mémorisé en elle et reçu du circuit 33, et le circuit d'interface 24 reste inutilisable.

De même, la saisie d'un mot de code incorrect d'accès au service XX interdit tout accès au service (34) et au réseau (24).

Ainsi, l'accès au service de transmission sécurisée d'informations est protégé par une clé matérielle, la carte à puce 4, et par une clé logicielle, le mot de code AB d'accès au réseau 1.

On remarquera cependant qu'il serait possible de ne prévoir qu'une seule des clés ci-dessus, matérielle ou logicielle, d'accès au service, que l'on commence par saisir sur le circuit 33 d'authentification de l'accès au service (34) avant d'établir la communication avec le réseau 1 par l'authentification de l'accès au réseau 1, qui se déduit de l'authentification de l'accès au service.

On remarquera aussi que le connecteur 32 pourrait être prévu solidaire du boîtier 20, afin de permettre aussi une utilisation non sécurisée du combiné 2. Il peut, encore, être prévu que le module de sécurité reconnaisse le mot de code d'accès au réseau AB et le transmette à la carte 4, le circuit d'embrouillage/débrouillage étant alors contourné pour établir la communication avec le réseau 1. Il aurait pu encore être prévu que ce soit le module 3, et non pas la carte 4, qui commande le bloc de communication 24, la carte 4 ne faisant alors fonction que de mémoire morte, sans circuit logique de comparaison commandant le bloc de communication 24.

L'ensemble 22 peut également être relié directement au bloc de communication 24 pour l'établissement de communications ne demandant pas d'authentification, comme par exemple un appel d'urgence.

REVENDICATIONS

1. Procédé de communication sur un réseau de transmission, au moyen d'un support de données (3, 4) personnel à un utilisateur et à double code d'authentification, l'un (AB) pour l'accès au réseau, l'autre (XX) pour l'accès à un service, caractérisé par le fait qu'on commence par saisir sur le support de données le code d'authentification de l'accès au service (XX) avant d'établir la communication par le code d'authentification de l'accès au réseau (AB) qui se déduit du code d'authentification de l'accès au service (XX).

2. Procédé selon la revendication 1, dans lequel le code d'authentification de l'accès au réseau (AB) se déduit du code d'authentification de l'accès au service (XX) par chiffrement.

3. Procédé selon l'une des revendications 1 et 2, dans lequel on valide le code d'authentification de l'accès au service (XX) par comparaison à un code d'authentification initiale d'accès au service, avant déduction du code d'authentification de l'accès au réseau (AB).

4. Procédé selon l'une des revendications 1 à 3, dans lequel on valide le code d'authentification de l'accès au réseau (AB) par comparaison à un code d'authentification initiale de l'accès au réseau (AB).

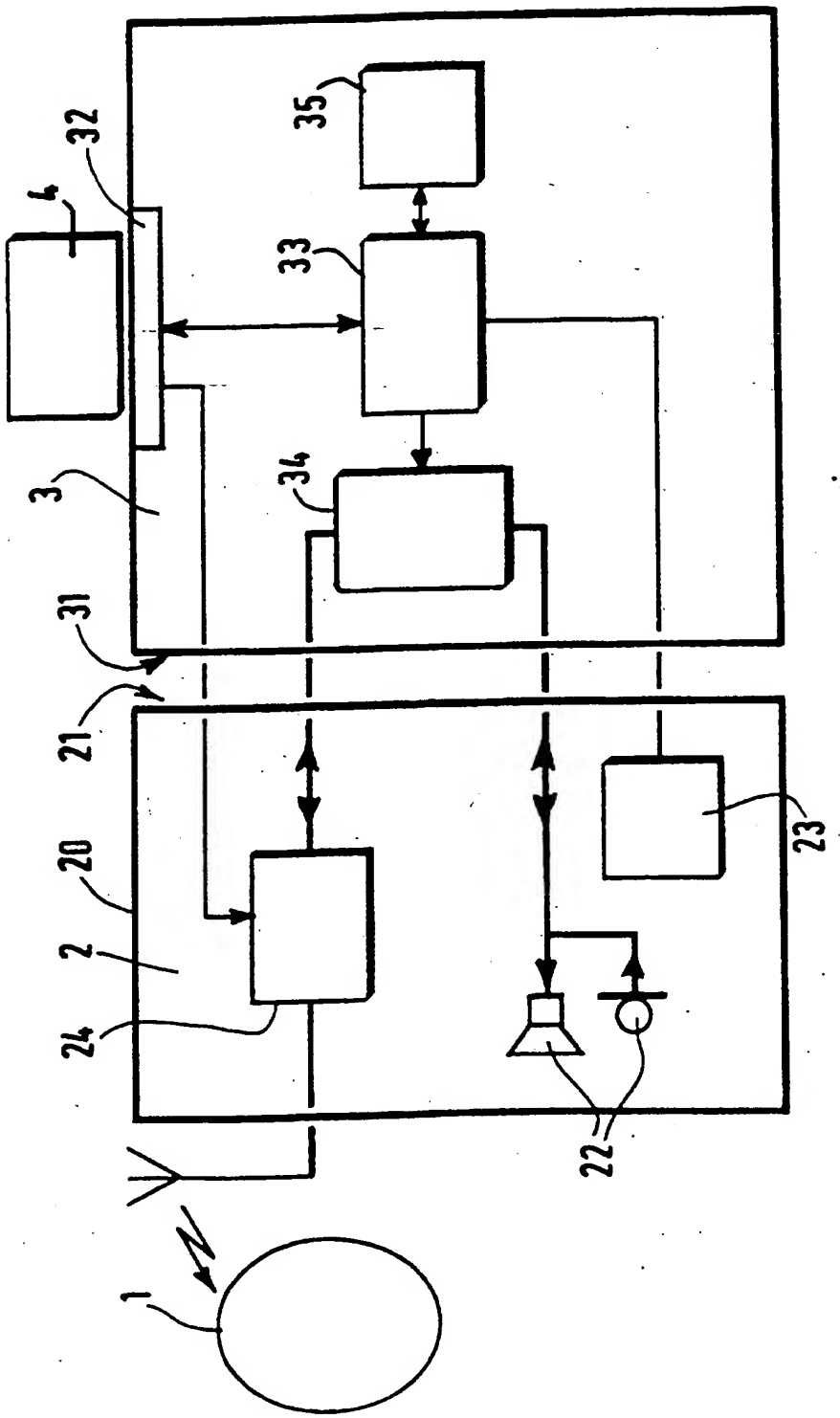
5. Procédé selon l'une des revendications 1 à 4, appliqué à la communication sur réseau GSM.

6. Support de données (3, 4) pour la mise en oeuvre du procédé de la revendication 1, comprenant un module d'accès au service (33) et un module d'accès au réseau (4), caractérisé par le fait qu'il comporte des moyens (33, 35) agencés pour déduire un code d'authentification (AB) de l'accès au réseau (1) d'un code d'authentification (XX) de l'accès au service (34) et pour commander le module d'accès au réseau (4).

7. Support de données selon la revendication 6, dans lequel le module d'accès au réseau (4) est un micromodule d'identification d'abonné (SIM).

8. Support de données (3) selon l'une des revendications 6 et 7, dans lequel le module d'accès au service (33) est associé à une mémoire (35) de stockage d'un code d'authentification de l'accès au service (XX).

9. Ensemble du support de données (3) de l'une des revendications 6 à 8 et d'un terminal de communication (2) comprenant une interface homme-terminal (23) et un bloc de communication (24), caractérisé par le fait que le module d'accès au réseau (4) du support de données (3) est relié directement au bloc de communication (24) du terminal (2).


35
32
4
33
3
34
31
21
20
2
24
23
22
1

REPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE PRELIMINAIRE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

2716319

N° d'enregistrement national

FA 499002
FR 9401680

DOCUMENTS CONSIDERES COMME PERTINENTS		Revendications concernées de la demande examinée
Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	
A	L'ECHO DES RECHERCHES, no.139, 1990, ISSY/MOULINEAUX (FR) pages 13 - 20, XP000386290 P.JOLIE & G.MAZZIOTTO 'UNE APPLICATION DE LA CARTE A MICROPROCESSOR: LE MODULE D'IDENTITE D'ABONNE DU RADIOTELEPHONE NUMERIQUE EUROPEEN' * page 14, colonne du milieu, ligne 28 - page 16, colonne de gauche, ligne 64 * ---	1,6,9

DOMAINES TECHNIQUES RECHERCHES (Int.Cl.5)

H04L
H04Q

Date d'achèvement de la recherche: 7 Novembre 1994

Examinateur: Lydon, M

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

1

EPO FORM 1503 03.82 (P04C13)